

The Honorable Robert S. Lasnik

UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

UNITED STATES OF AMERICA,

Plaintiff

v.

PAIGE A. THOMPSON,

Defendant.

NO. CR19-159 RSL

**UNITED STATES' OPPOSITION
TO DEFENDANT'S MOTION TO
DISMISS COUNTS 1, 9, AND 10 OF
THE SUPERSEDING INDICTMENT**

I. INTRODUCTION

The multi-count superseding indictment charging Defendant Paige Thompson with computer crimes related to hacking and cryptojacking gives her fair notice of the wire fraud charge (Count 1), access device fraud (Count 9), and aggravated identity theft (Count 10), as required by the Federal Rules of Criminal Procedure. Under Rule 7(c)(1), the indictment “must be a plain, concise, and definite written statement of the essential facts constituting the offense charged.” The Ninth Circuit has repeatedly held that “an indictment setting forth the elements of an offense is generally sufficient.” *United States v. Fernandez*, 388 F.3d 1199, 1219 (9th Cir. 2004) (citing *United States v. Woodruff*, 50 F.3d 673, 676 (9th Cir. 1995)). Here, the indictment goes further, alleging specific acts Thompson took in furtherance of her scheme to defraud the victims of money or property by means of false and fraudulent pretenses and representations. The indictment provides more than enough

information for Thompson to know the nature of the accusations against her and prepare to meet them. Accordingly, her motion to dismiss Counts 1, 9, and 10 of the indictment should be denied. Thompson also has enough information, not only from the face of the indictment but also from the discovery produced to-date—including grand jury transcripts and exhibits—to obviate the need for a bill of particulars. Thompson is entitled to know the theory of the government’s case, not the details of how it is intended to be proved. The Court should deny Thompson’s request for a bill of particulars.

II. BACKGROUND

A. The indictment thoroughly describes the charged conduct

The underlying facts of this case are outlined in Part II of the United States’ Opposition to Defendant’s Motion to Strike Cryptojacking Allegations and to Sever Count 8, and are incorporated herein by reference. As relevant to this motion, the ten-count superseding indictment returned by the grand jury contains a concise and definite statement of the wire fraud charge.¹ *See* Dkt. No. 102. It alleges that:

Beginning in or before March 2019, and continuing until on or about July 17, 2019, at Seattle, within the Western District of Washington, and elsewhere, PAIGE A. THOMPSON, with the intent to defraud, devised and intended to devise, a scheme and artifice to defraud and to obtain money and property by means of materially false and fraudulent pretenses, representations, and promises.

Id., ¶ 1. The indictment then includes 21 additional paragraphs of information about the scheme, setting forth the victims, the object of the scheme, the manner and means employed, and Thompson’s execution of the scheme. *See id.*, ¶¶ 2–22.

In describing the materially false and fraudulent pretenses and representations Thompson made in furtherance of the scheme, the indictment states that Thompson “implicitly represented that commands to copy data that she sent using the accounts for

¹ As explained in the Opposition to Defendant’s Motion to Strike Cryptojacking Allegations and to Sever Count 8, the government intends to file a second superseding indictment to further clarify certain facts alleged in the first superseding indictment. Because the planned changes (as shown in the draft filed with the government’s opposition to the motion to strike) are not material to the motion—if anything, they add slight additional detail to the indictment—this opposition addresses the wire fraud count as alleged in the first superseding indictment.

1 which she had obtained security credentials were legitimate commands sent by users with
 2 permission to send such commands, rather than commands sent by a person who had stolen
 3 the security credentials and who lacked authority to use the accounts and send the
 4 commands.” *Id.*, ¶ 16. The indictment also describes the steps Thompson took to hide her
 5 location and identity, *see id.*, ¶¶ 17–18 (discussing use of VPNs and TOR), provides the
 6 specific date on which Thompson transmitted by means of wire communication in
 7 interstate commerce a command to copy data belonging to Capital One from its rented
 8 servers to her own server, *see id.*, ¶ 22, and explains that in addition to using security
 9 credentials to obtain property, Thompson used them to employ the stolen computing power
 10 of victim servers to “mine” cryptocurrency for her own benefit, *see id.*, ¶¶ 15, 21.²

11 **B. The government has provided full discovery**

12 Since 2019, the government has provided comprehensive electronic discovery (over
 13 13,500 Bates-numbered pages, including placeholder pages for the digital material
 14 provided), which gives Thompson substantial information about the charges and the
 15 government’s case. The productions include both searchable native and image files, as well
 16 as detailed production logs. On October 4, 2019, the government met with counsel for
 17 Thompson and delivered a 38-page PowerPoint detailing its investigation. The government
 18 subsequently gave Thompson’s counsel a copy of the PowerPoint (attached as Exhibit A).
 19 The presentation provides the information Thompson appears to seek in her request for a
 20 bill of particulars, including specific instances of Thompson’s unauthorized use of security
 21 credentials, the dates when those credentials were used, the data that was exfiltrated
 22 through their use, and the computer scripts Thompson employed to search for and copy
 23 data as well as to mine cryptocurrency. On November 23, 2021, far in advance of any
 24 requirement to produce such *Jenks* material, the government produced grand jury
 25 transcripts and exhibits which allow Thompson to see exactly what evidence the grand jury
 26 reviewed in returning the original and superseding indictments.

27
 28 ² The indictment also lists five more dates on which Thompson used stolen security credentials to access
 the servers of other victim entities to obtain information. *See id.*, ¶¶ 26–27.

1 A defendant may move to dismiss an indictment for “lack of specificity” or “failure
 2 to state an offense.” Fed. R. Crim. P. 12(b)(3)(B). In evaluating such a motion, the Court
 3 must accept the allegations in the indictment as true and is “bound by the four corners of
 4 the indictment . . . in analyzing whether a cognizable offense has been charged.” *United*
 5 *States v. Boren*, 278 F.3d 911, 914 (9th Cir. 2002). However, the indictment “should be
 6 read in its entirety, construed according to common sense, and interpreted to include facts
 7 which are necessarily implied.” *United States v. Berger*, 473 F.3d 1080, 1103 (9th Cir.
 8 2007) (internal quotation marks and citation omitted). A Rule 12(b)(3)(B) motion is
 9 “capable of determination before trial if it involves questions of law rather than fact” and
 10 therefore does not intrude upon “the province of the ultimate finder of fact.” *United States*
 11 *v. Kelly*, 874 F.3d 1037, 1046–47 (9th Cir. 2017) (quotations omitted).

12 Under Federal Rule of Criminal Procedure 7(f), a court “may direct the government
 13 to file a bill of particulars.” However, a bill of particulars is appropriate only when an
 14 indictment is too vague or indefinite to inform the defendant of the charges, permit the
 15 preparation of an adequate defense, or allow double jeopardy to attach. *See Giese*, 597 F.2d
 16 at 1180. Courts in this Circuit consider whether the defendant has been adequately advised
 17 of the charges through the indictment and *all other disclosures made by the government.*”
 18 *United States v. Long*, 706 F.2d 1044, 1054 (9th Cir. 1983) (emphasis added). “Full
 19 discovery . . . obviates the need for a bill of particulars.” *Giese*, 597 F.2d at 1180.

20 **B. Thompson misunderstands the superseding indictment’s wire fraud**
 21 **allegations and misstates what the government must allege**

22 Thompson purports to misunderstand the materially false pretenses and
 23 representations alleged in Count 1 of the superseding indictment. To be clear, contrary to
 24 Thompson’s suggestion, *see* Dkt. No. 122 at 6, the government is not claiming that the use
 25 of a proxy scanner in this case is a misrepresentation, nor that using a VPN or TOR to
 26 conceal one’s IP address, standing alone, necessarily constitutes the concealment of a
 27 material fact. The government’s position, and what the indictment clearly alleges, is that
 28 in carrying out her scheme and artifice to defraud and to obtain money and property,

Thompson “implicitly represented that commands to copy data that she sent using the

accounts for which she had obtained security credentials were legitimate commands sent by users with permission to send such commands, rather than commands sent by a person who had stolen the security credentials and who lacked authority to use the accounts and send the commands.” Dkt. No. 102, ¶ 16. The same is true for Thompson’s use of stolen security credentials to access victim servers to mine cryptocurrency, consuming large amounts of computing power and hardware. *See id.*, ¶ 21. The act of accessing a server with stolen credentials itself is a materially false pretense and representation. *See, e.g., United States v. Khalupsky*, 5 F.4th 279, 291 (2d Cir. 2021) (in securities fraud case requiring proof of a scheme or artifice to defraud in connection with the purchase or sale of any security, holding that “[e]very time the hackers attempted to access parts of the system by entering stolen credentials, they misrepresented themselves to be authorized users” and “misrepresenting one’s identity in order to gain access to information that is otherwise off limits, and then stealing that information is plainly deceptive within the ordinary meaning of the word” (internal quotation marks and citation omitted)).

In any event, the indictment also sufficiently alleges a wire fraud charge because it alleges “a scheme or artifice to defraud,” which the Ninth Circuit has held “may or may not involve any specific false statements.” *United States v. Woods*, 335 F.3d 993, 999 (9th Cir. 2003) (after the Supreme Court’s decision in *Neder v. United States*, 527 U.S. 1 (1999), rejecting the requirement that a mail fraud charge must include “a specific false statement or a specific omission” because “there are alternative routes to a mail fraud conviction, one being proof of a scheme or artifice to defraud” (internal citation omitted));³ *see also United States v. Holmes*, 2020 WL 666563, at *6 (N.D. Cal. Feb. 11, 2020) (denying motion to dismiss wire fraud charges because “the Government need not allege specific misstatements to meet the ‘fair notice’ requirement”). Under either approach to proving wire fraud, the indictment in this case provides Thompson with fair notice under Rule 7(c)(1).

³ Cases construing the mail fraud and wire fraud statutes are applicable to either. *See Carpenter v. United States*, 484 U.S. 19, 25 n.6 (1987).

Thompson’s use of a VPN and TOR to conceal her location and identity were part of the scheme that *allowed* her to falsely represent that the commands she sent came from a user with authority to use the stolen security credentials. And, as discussed further below, her use of those services supports the inference that she specifically intended to defraud the victims. The government is not, as Thompson claims, trying to “slap together a number of innocuous technical processes . . . to gin up a wire fraud charge” against her. Dkt. No. 122 at 6. Rather, the government has alleged facts that establish the elements of wire fraud, namely: “(1) the existence of a scheme to defraud; (2) the use of wire, radio, or television to further the scheme; and (3) a specific intent to defraud.” *United States v. Jinian*, 725 F.3d 954, 960 (9th Cir. 2013).

Thompson also states, without any support, that “the copying of data, without knowing what those datasets contain cannot establish an intent to deceive and cheat.” Dkt. No. 122 at 6. She further claims that “utilizing a public computer server (even one that was made public through the mistake of its owner and/or renter) to mine cryptocurrency” likewise does not establish the requisite intent. *Id.* As to the former point, whether or not Thompson knew what she was downloading perhaps may be a defense she can raise at trial based on facts presented to the jury, not an argument to dismiss Count 1 of the indictment as a matter of law. *See Kelly*, 874 F.3d at 1046 (questions of law but not of fact are “capable of determination before trial”). And as to the latter point, the indictment does not allege that Thompson mined cryptocurrency using a publicly available server; rather, it alleges that Thompson used her *unauthorized access* to certain victim servers (obtained through stolen security credentials) to steal the computing power of those servers to mine cryptocurrency. Dkt. No. 102, ¶ 21. Thompson’s arguments on these points are not reasons to dismiss under Rule 12(b)(3)(B).

Next, Thompson states several times in her motion that the superseding indictment “fails to describe how [she] purportedly intended to cause any amount of loss to *any* of the alleged victims.” Dkt. No. 122 at 1; *see also id.* at 9 (arguing the need for “facts sufficient to demonstrate that she intended to cause loss to each and every separate victim alleged in

Count 1”). Again, these statements of what the government must allege to make out a wire fraud charge are incorrect. In order “to be guilty of wire fraud, a defendant must act with the intent . . . to deprive a victim of money or property by means of” false statements or other forms of deception, *United States v. Miller*, 953 F.3d 1095, 1101 (9th Cir. 2020), but “it is not necessary to show that the scheme was successful or that the intended victim suffered a loss or that the defendants secured a gain,” *Schreiber Distrib. Co. v. Serv-Well Furniture Co.*, 806 F.2d 1393, 1400 (9th Cir. 1986) (emphasis added); *see also United States v. Louderman*, 576 F.2d 1383, 1387 (9th Cir. 1978) (same). Here, the indictment needed to allege that Thompson acted with the intent to defraud—that is, with the intent to deprive the victims of money or property⁴—not that she intended to cause them specific amounts of loss. The indictment in this case meets this standard.

To satisfy the intent element, the indictment not only alleged that Thompson engaged in a scheme to defraud as set forth in the wire fraud statute, but alleged further facts demonstrating her specific intent to defraud. *See United States v. Lothian*, 976 F.2d 1257, 1267–68 (9th Cir. 1992) (fraudulent intent can be inferred from “a pattern of conduct or a series of acts, aptly designated as badges of fraud,” including misrepresentations). Thompson’s intent to defraud can be inferred from multiple factual allegations in the indictment about her pattern of conduct, including: (1) creating and using scanners that allowed her to identify servers with misconfigured web application firewalls, Dkt. No. 102, ¶ 12; (2) “transmitti[ng] commands to the misconfigured servers that obtained the security credentials for particular accounts or roles belonging” to the victims, *id.*, ¶ 13; (3) using the security credentials “to obtain lists or directories of folders” of data on the victims’ cloud storage space, *id.*, ¶ 14; (4) using the stolen credentials “to copy data, from folders or buckets of data” in the victims’ cloud storage space, *id.*, ¶ 15; (5) implicitly representing

⁴ The data Thompson downloaded constitutes property under the wire fraud statute. *See Carpenter*, 484 U.S. at 25 (the “intangible nature” of “confidential business information” “does not make it any less ‘property’ protected by the mail and wire fraud statutes”); *Louderman*, 576 F.2d at 1387 (affirming wire fraud conviction where “[t]he object of the scheme to defraud . . . was . . . to obtain intangible, commercial information which the telephone company and post office chose to keep confidential and which its customers expected would remain confidential”).

1 that the commands she sent to the servers were legitimate and came from a user with
 2 permission to send such commands, *id.*, ¶ 16; (6) using VPNs and TOR to conceal her
 3 location and identity while taking these actions, *id.*, ¶¶ 17–18; and (7) using “her
 4 unauthorized access to certain victim servers—and stolen computing power of those
 5 servers—to ‘mine’ cryptocurrency for her own benefit,” *id.*, ¶ 21. All of these actions
 6 support a strong inference of intent to deprive the victims of money or property. The
 7 indictment is more than sufficient on this point, and the Court should reject any suggestion
 8 by Thompson that an indictment for wire fraud must further allege an intent to cause a
 9 specific amount of loss to the victims of the fraud.⁵

10 The superseding indictment here suffers from none of the shortcomings identified
 11 in the cases Thompson cites in her motion. In *United States v. Du Bo*, for example, the
 12 indictment alleged the wrong *mens rea* for a Hobbs Act charge, 186 F.3d 1177, 1179 (9th
 13 Cir. 1999). In *United States v. King*, 587 F.2d 956, 963–64 (9th Cir. 1978), the indictment
 14 failed to charge an essential element of the drug offense, i.e., that the doctor who dispensed
 15 the cocaine did so without authorization. In *Cecil*, the indictment included “only two
 16 specific allegations concerning the [drug] conspiracies,” failed “to state any other facts or
 17 circumstances pertaining to the conspiracy or any overt acts done in furtherance thereof,”
 18 and failed “to place the conspiracies within any timeframe.” 608 F.2d at 1297; *see also id.*
 19 (the timeframe was “open-ended in both directions” because it alleged the conspiracy
 20 began “on or before July, 1975” and continued “until on or after October, 1975” (emphasis
 21 added)). And in *United States v. Curtis*, 506 F.2d 985, 989 (10th Cir. 1974), and *United*
 22 *States v. Keuylian*, 23 F. Supp. 3d 1126, 1128 (C.D. Cal. 2014), the indictments did not
 23 state how the schemes at issue were false and fictitious. *See also Keuylian*, 23 F. Supp. 3d
 24 at 1128 (noting the indictment “fail[ed] to describe *any* act of deception committed by” the
 25 defendant (emphasis added)). Finally, the indictment in *United States v. Steffen*, 687 F.3d
 26

27
 28 ⁵ The Court also should reject any suggestion that at this stage the government must outline its evidence in support of these allegations. *See Buckley*, 689 F.2d at 897, 899 n.5

1 1104, 1117 (8th Cir. 2012), was deficient because on the facts alleged, the defendant “made
 2 no false representation, submitted no misleading or falsified documents, and took no
 3 affirmative steps to conceal” what he had done.

4 The indictment in this case meets the requirements of Rule 7(c)(1) and gives
 5 Thompson enough information to know the nature of the accusations against her. *See* Dkt.
 6 No. 102, ¶¶ 1–22 (detailing the essential elements of the scheme, its object, the manner and
 7 means employed, and how the scheme was executed). Accordingly, the Court should deny
 8 Thompson’s request to dismiss Count 1 of the superseding indictment. And, because
 9 Thompson has not argued any reason to dismiss Counts 9 and 10 beyond that they are
 10 founded on Count 1, the Court also should reject her request to dismiss those counts.

11 **C. A bill of particulars is unnecessary because the indictment satisfies Rule 7**
 12 **and the government has provided substantial discovery**

13 The Court should deny Thompson’s request for a bill of particulars under Rule 7(f).
 14 As set forth above, the superseding indictment satisfies the government’s obligations under
 15 Rule 7. *See Giese*, 597 F.2d at 1180 (“To the extent that the indictment or information itself
 16 provides details of the alleged offense, a bill of particulars is, of course, unnecessary.”
 17 (citation omitted)). But even if Thompson needed additional “clarification in order to
 18 prepare a defense,” the Court should consider “all other disclosures made by the
 19 government.” *Long*, 706 F.2d at 1054 (citing *Giese*, 597 F.2d at 1180). Thompson has been
 20 given considerable additional information in this case, including at a meeting during which
 21 the government detailed its investigation, through production of searchable, indexed
 22 electronic discovery, and via disclosure of grand jury transcripts and exhibits. Thompson’s
 23 request for the “when, where, and how” of every act she took in furtherance of her scheme
 24 to defraud “is not a purpose of the bill of particulars,” *Giese*, 597 at 1181, but even if it
 25 was, that information is already available in the material the government has produced to
 26 her.⁶

27
 28 ⁶ Notably, Thompson has deliberately failed to avail herself of all the discovery available to her under Rule
 16. *See* Dkt. No. 125 (government’s motion explaining that Thompson has not requested expert discovery in order to
 avoid the obligation to provide reciprocal discovery). The Court should not permit Thompson to use a bill of particulars
 UNITED STATES’ OPPOSITION TO DEFENDANT’S
 MOTION TO DISMISS COUNTS 1, 9, AND 10
United States v. Thompson / CR19-159 RSL - 10
 UNITED STATES ATTORNEY
 700 STEWART STREET, SUITE 5220
 SEATTLE, WASHINGTON 98101
 (206) 553-7970

Thompson objects that the discovery provided by the government is too “voluminous,” *see* Dkt. No. 122 at 7, but the cases she cites in support of this argument are distinguishable and she ignores numerous cases from this Circuit concluding that providing discovery—especially when it includes grand jury materials or is electronically searchable—is “sufficient to enable [a defendant] to prepare [her] defense for trial.” *United States v. Ayers*, 924 F.2d 1468, 1484 (9th Cir. 1991). Thompson relies on *United States v. Bortnovsky*, 820 F.2d 572, 575 (2d Cir. 1987) (*per curiam*), but there, new counsel in the case “had only four days within which to prepare a defense,” and “providing mountains of documents to defense counsel” was not sufficient to help him sort through “which of some fifteen burglaries would be demonstrated to be staged.” In *United States v. Feil*, 2010 WL 1525263, at *3 (N.D. Cal. Apr. 15, 2010), the court granted a motion for a bill of particulars in part but noted that—unlike in Thompson’s case—the alleged conspiracies “span[ned] a period of three to seven years,” the government produced “over 70,000 pages of discovery,” and it was “not clear to the Court that all discovery disputes between the parties ha[d] been resolved.” And in *United States v. Nachamie*, 91 F. Supp. 2d 565, 571 (S.D.N.Y. 2000), discovery was not provided electronically (the government “produced over 200,000 pieces of paper in hundreds of boxes and files, relating to 2,000 Medicare claims”).⁷

None of those circumstances are present here. Instead, this case resembles *United States v. Hsuan Bin Chen*, 2011 WL 332713, at * 8 (N.D. Cal. Jan. 29, 2011) (declining to order a bill of particulars because “[w]hile the discovery is voluminous, the government has provided it in a fashion designed to help defendants prepare their defense,” the government “began production of discovery as soon as the defendants and the Court signed a protective order,” the “government conducted separate meetings with defense counsel,”

as a mechanism for an end-run around Rule 16. *See, e.g., United States v. W.R. Grace*, 401 F. Supp. 2d 1103, 1106 (D. Mont. 2005) (“Rule 7(f) is not intended as a vehicle for obtaining discovery from the government.”).

⁷ *United States v. Trumpower*, 546 F. Supp. 2d 849, 852 (E.D. Cal. 2008), and *United States v. Sampson*, 448 F. Supp. 2d 692, 696 (E.D. Va. 2006), are also distinguishable because those indictments lacked important details, and *United States v. Bazezew*, 783 F. Supp. 2d 160, 168 (D.D.C. 2011), merely states, without any analysis or description of what was produced, that pointing to voluminous discovery alone is not a sufficient response to a request for a bill of particulars.

and the government “indexed both hard copy and electronic documents, and produced electronic discovery in a searchable format”). *See also United States v. Lillard*, 2016 WL 11683870, at *1 (W.D. Wash. Dec. 16, 2016) (denying bill of particulars where the government provided full discovery and a presentation with information specific to the defendant’s alleged involvement in the charged offenses); *United States v. Hunter*, 2009 WL 10681101, at *3 (C.D. Cal. June 8, 2009) (no bill of particulars needed where defendant “received voluminous discovery including grand jury transcripts setting forth the entire basis of the prosecution against her”). Thompson has been adequately advised of the charges against her through the indictment and all other disclosures made by the government. A bill of particulars for Count 1 is not necessary.

D. Conclusion

For the foregoing reasons, the United States respectfully requests the Court deny Thompson’s motion to dismiss Counts 1, 9, and 10 of the superseding indictment and deny her request for a bill of particulars as to Count 1.

DATED: December 23, 2021.

Respectfully submitted,

NICHOLAS W. BROWN
United States Attorney

s/ Andrew Friedman

s/ Jessica M. Manca

ANDREW FRIEDMAN

JESSICA M. MANCA

Assistant United States Attorney

700 Stewart Street, Suite 5220

Seattle, WA 98101-1271

Telephone: (206) 553-7970

Fax: (206) 553-0882

E-mail: Andrew.Friedman@usdoj.gov

Jessica.Manca@usdoj.gov